

REMARKS

Claims 1-3, 7-13, 17-24, and 27-30 are pending. By this Amendment, claims 11-13, 17-24 and 27-30 are amended.

Objections to the Claims

Claims 21-24 and 27-30 have been objected to for informalities. By this Amendment, any causes of these objections have been remedied. Withdrawal of the objections is respectfully requested.

Claim Rejections under 35 U.S.C. § 101

Claims 11-20 have been rejected as being directed to non-statutory subject matter because they are directed to program instructions. Amended claim 11 and its dependents now claim a system for adding copy protection to a program, the system comprising a computing device programmed to perform the stated functions. Applicant respectfully points out that a system comprising a computing device is a “machine” within the meaning of 35 U.S.C. § 101. Withdrawal of the § 101 rejection is respectfully requested.

Claim Rejections under 35 U.S.C. § 102 and § 103

Claims 1, 3, 7, 9-11, 13, 17, 19-21, 23-24, 27, and 29-30 have been rejected under Section 102(b) as being anticipated by U.S. Patent No. 6,266,416 to Sigbjornsen et al. (hereinafter, “Sigbjornsen”). Claims 2, 12, and 22 have been rejected under Section 103(a) as being obvious in view of Sigbjornsen, and further in view of U.S. Pat. No. 5,343,524 to Mu et al. For at least the reasons provided below, these rejections are respectfully traversed.

Sigbjornsen is directed to a software protection technique in which at least one portion of a computer program is encrypted. During execution, when an encrypted portion of the program

is reached, the program must communicate with a Smart Card. The Smart Card holds a cryptographic algorithm and a private access key, and is adapted to receive encrypted information from the computer program and decrypt the information using one or more algorithms and/or keys stored on the Smart Card, allowing the software to continue to be executed as part of the program in the main computer

The protection is provided by the insertion, in different locations of the software, of program calls to the Smart Card, or to special software at the disposal to the card, thereby obtaining the information necessary to proceed correctly in the execution of the protected program. For example, this information may be certain parameters which are used when the program is executed, and which is determined by those who wish to protect their software.

Sigbjornsen et al., column 5 line 66-column 6, line 3.

At the moment the execution reaches an encrypted parameter ($(g(10)$ in the example shown) the value $(g(10)+T)$) is sent to the special software which further conveys $f(g(10)+T)-T$ to the Smart Card. In the Smart Card, the value of $g^{-1}((10)+T)-T$, and this value is returned to the special software. By means of the special software $f(g^{-1}((10)+T)-T)$ is then calculated, this being equal to x and $x+T$; and this result is supplied to the protected program as parameter C for the utilization in the program.

Sigbjornsen et al., column 7 lines 15-24.

In contrast, the invention claimed in claims 1, 11, and 21 is directed to making a computer program copy-protected by converting a decision section of the program to produce a copy-protected version of the code. The converting includes providing code in the copy-protected version of the program, which includes data and a processing regulation applicable to the data for execution of the decision section. The code is *executable exclusively on a copy protection unit*.

“Executing” the code exclusively in the copy protection unit as claimed in claims 1, 11, and 21 implies that the program logic corresponding to the converted decision section be carried out in the copy protection unit, and not in the computing section. Sigbjornsen et al. discloses execution of a *decryption algorithm* stored on a Smart Card (and not execution of the program logic itself in the smart card) in order to enable execution of otherwise encrypted portions of the computer program in the main computer. Applicant respectfully points out that simply decrypting or converting a portion of the program by a processor in the smart card and returning

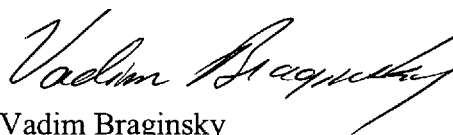
the decrypted or converted portion for further use in the main computer, as disclosed in Sigbjornsen et al., cannot fairly be construed as *executing* the code *exclusively* in the copy protection unit as claimed in claims 1, 11, and 21.

For at least these reasons, independent claims 1, 11, and 21 are believed to be allowable over Sigbjornsen et al. Each of dependent claims 2-3, 7-10, 12-13, 17-20, 22-24, and 27-30 further limits its respective base claim; therefore, these claims are also believed to be allowable. Withdrawal of the § 102 and § 103 rejections is respectfully requested.

In view of the foregoing, it is submitted that this application is in condition for allowance. Favorable consideration and prompt allowance of the application are respectfully requested.

The Examiner is invited to telephone the undersigned if the Examiner believes it would be useful to advance prosecution.

Respectfully submitted,



Vadim Braginsky
Registration No. 58, 031

Customer No. 24113
Patterson, Thunte, Skaar & Christensen, P.A.
4800 IDS Center
80 South 8th Street
Minneapolis, Minnesota 55402-2100
Telephone: (612) 252-1542